# National Infrastructure Protection Center CyberNotes

*Issue #2000-08* *April 26, 2000*

**CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.**

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

## *Bugs, Holes & Patches*

The following table provides a summary of software vulnerabilities identified between April 10 and April 20, 2000. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| AdTran Inc.[1] | MX2800 M13 | A Denial of Service vulnerability exists when the network interface is flooded. All connections are dropped and services are unavailable. | No workaround or patch available at time of publishing. | AdTran Ping Flood Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| AVM[2]<br><br>Windows 95/98 NT 4.0 | KEN! 1.4.30, 1.3.10, 1.4.32 | Two security Vulnerabilities exist. One allows a remote malicious user to cause a Denial of Service attack, and the other allows downloading of any file. | AVM has released version 1.04.32 which does not have this vulnerability. Contact AVM for download instructions. | AVM KEN! 1.3.10 Directory Traversal | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[1] Bugtraq, April 20, 2000.
[2] NTSecurity, April 19, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Be Incorporated[3]<br><br>Windows 95/98/2000 NT4 | BeOS 5.0, 4.5 | A vulnerability exists which crashes the system when certain malformed packets are sent. | Be has marked the bug as "Will Not Fix" with the comment "The entire networking system will be replaced soon." | BeOS 4.5/5.0 Invalid System Call | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Bray Systems[4]<br><br>Unix | Linux Trustees 1.5 and prior | The Trustees kernel makes the Linux machine vulnerable to a Denial of Service attack. | Linux Trustees 1.6 has been released which eliminates this vulnerability. It can be downloaded at: http://www.braysystems.com/linux/trustees.html | Bray Systems Trustees Long Pathname Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Cisco Systems[5] | IOS Software 11.3AA, 12.0 releases: 12.0(2) up to and including 12.0(6) and 12.0(7) | A vulnerability exists in the Telnet Environment handling code, which causes the Cisco router to reload unexpectedly when the router is tested for security vulnerabilities by security scanning software programs. The defect can be exploited repeatedly to produce a consistent Denial of Service attack. | For workaround see the Cisco Security Advisory on this issue at: www.cisco.com | Cisco IOS Software TELNET Option Handling | Low/ **High**<br><br>**(High if DDoS best-practices not in place)** | Bug discussed in newsgroups and websites. **Numerous security scanners are available and carry out this attack.** |
| Cisco Systems[6] | Catalyst 4000, 5000, 5500, 6000, 6500 5.4.1 | A vulnerability exists, which permits unauthorized access to the enable mode. Once initial access is granted, access can be obtained for the higher level "enable" mode without a password. | This problem is resolved in version 5.4(2) which can be found at: http://www.cisco.com. | Cisco Catalyst Enable Password Bypass | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| CNC Technology[7] | BizDB 1.0 | A vulnerability exists in the bizdbsearch.cgi, which could allow a malicious user to execute commands at the privilege level of the webserver. | No workaround or patch available at time of publishing. | BizDB bizdb-search.cgi Remote Command Execution | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| CRYPTOCard[8]<br><br>Multiple systems | CRYPTO Admin 4.1 | A vulnerability exists, which could allow a malicious user to determine the private PIN number of a users token and clone the challenge/response scheme of the legitimate user. | No workaround or patch available at time of publishing. | CRYPTOCard Weak Encryption | Medium | Bug discussed in newsgroups and websites. Exploits scripts have been published. |

[3] Bugtraq, April 10, 2000.
[4] Bugtraq, April 10, 2000.
[5] Cisco Security Advisory, CI-00.03, April 19, 2000.
[6] Cisco Security Advisory, CI-00.02, April 19, 2000.
[7] Securiteam, April 10, 2000.
[8] L0pht Research Labs Security Advisory, April 10, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Dansie[9]<br><br>Multiple platforms | Shopping Cart 2.84, 3.03, 3.04 | Multiple vulnerabilities exist, which allow arbitrary commands to be executed on the victim server. Remote malicious users can display the configuration settings of the application (includes username and password used for credit card transactions), and list the entire database file containing all items in the shopping cart. Also contains obscured Perl codes that send e-mails, containing sensitive information, back to the author. | The Dansie Shopping Cart bug, which sends e-mail messages back to the author, has been removed. | Dansie Shopping Cart Multiple Vulnerabilities | **High** | Bug discussed in newsgroups and websites. Exploits have been published. Vulnerabilities have appeared in the Press. |
| FreeBSD[10]<br><br>Unix | Generic-NQS versions 3.50.7 and earlier | A security vulnerability exists which could allow a local malicious user to obtain root privileges. | Upgrade your entire ports collection and rebuild the generic-nqs port located at: ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/ | NQS | **High** | Bug discussed in newsgroups and websites. |
| Hewlett-Packard[11] | JetDirect J3111A rev. G.08.03, G.07.17, G.07.03, A.08.06 | A Denial of Service vulnerability exists in HP printers equipped with JetDirect cards. | No workaround or patch available at time of publishing. | JetDirect Portscan Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |
| Infonautics[12] | Infonautics applications | Applications which utilize the getdoc.cgi CGI contain a vulnerability which allows malicious users to gain read access to a document that they would have to pay in order to view. | No workaround or patch available at time of publishing. | Infonautics Getdoc.cgi Access | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| FreeBSD [13]<br><br>Unix | FreeBSD 4.0 (healthd 0.1-0.3) | A security vulnerability exists, which could allow local malicious users on the machine to gain root access. | The vulnerability has been patched in the latest version of healthd, available at: http://healthd.thehousleys.net/ | Healthd Buffer Overflow | **High** | Bug discussed in newsgroups and websites. |
| Microsoft[14]<br><br>Windows 2000 | Windows 2000 Server; Advanced Server | A security vulnerability exists which could, under very specific conditions, allow a malicious user to change information in the Active Directory. | Patch available at: http://www.microsoft.com/Downloads/Release.asp?ReleaseID=20490 | Mixed Object Access | Medium | Bug discussed in newsgroups and websites. |

[9] Bugtraq, April 11, 2000.
[10] FreeBSD-SA-00:13, April 19, 2000.
[11] Bugtraq, April 20, 2000.
[12] Securiteam, April 11, 2000.
[13] FreeBSD-SA-00:12, April 10, 2000.
[14] Microsoft Security Bulletin, MS-0026, April 20, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Microsoft[15]<br><br>Windows NT 4.0/2000 | Internet Information Server (IIS) 4.0, 5.0 | A vulnerability exists, which could allow a malicious user to slow a web server's response or prevent it from providing service for a period of time. | Patches can be found at:<br>Microsoft IIS 5.0:<br>http://download.microsoft.com/download/win2000platform/Patch/Q254142/NT5/EN-US/Q254142_W2K_SP1_x86_en.EXE<br>Microsoft IIS 4.0:<br>http://download.microsoft.com/download/iis40/Patch/4.2.740.1/NT4ALPHA/EN-US/escseq4a.exe | Microsoft Myriad Escaped Characters | Low | Bug discussed in newsgroups and websites. |
| Microsoft[16]<br><br>Windows 95/98<br>NT 4.0 | FrontPage | Three security vulnerabilities exist: 1) Gives a malicious user the full path to the root directory;<br>2) Simple buffer overflow;<br>3) Allows access files to any file. | No workaround or patch available at time of publishing.<br><br>Unofficial workaround:<br>If you are not using image maps on your website, htimage.exe can be deleted. | FrontPage htimage.exe Buffer Overflow | **High** | Bug discussed in newsgroups and websites.<br>Exploit has been published. |
| Microsoft[17]<br><br>Windows 9x<br>NT 4.0 | Visual Interdev 1.0 | DVWSSR.dll contains a security vulnerability that allows remote malicious users to cause IIS to stop responding. The buffer overflow can be used to execute arbitrary code on the remote server.<br><br>**NOTE:** Visual Interdev is a server-side component and is included in Windows NT 4.0 Option Pack, Personal Web Server 4.0 which ships as part of Windows 95/98, and FrontPage 98 Server Extensions | For workaround please see Microsoft Security Bulletin (MS00-025) Frequently Asked Questions located at:<br>http://www.microsoft.com/technet/security/bulletin/fq00-025.asp | Microsoft Link View Server-Side Component | **High** | Bug discussed in newsgroups and websites.<br>Exploit scripts have been published.<br>Vulnerability has appeared in the Press. |

[15] Microsoft Security Bulletin, MS00-023, April 12, 2000.
[16] Securiteam, April 20, 2000.
[17] Microsoft Security Bulletin, MS00-025, April 17, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Microsoft[18]<br><br>Windows NT 4.0 | Windows NT Terminal Server, NT 4.0 | A vulnerability exists in the default permissions which could allow a malicious user, who can interactively log onto a Windows NT 4.0 machine, to compromise the cryptographic keys of other users who subsequently log onto the same machine. | Microsoft has released a tool which addresses this vulnerability available at:<br>Microsoft Windows NT 4.0:<br>http://download.microsoft.com/download/winntsp/Patch/Q259496/ALPHA/EN-US/Q259496a.exe<br>Alpha<br>http://download.microsoft.com/download/winntsp/Patch/Q259496/NT4/EN-US/Q259496i.exe<br>Microsoft Windows NT Terminal Server:<br>http://download.microsoft.com/download/winntsp/Patch/Q259496/ALPHA/EN-US/Q259496a.exe<br>Alpha<br>http://download.microsoft.com/download/winntsp/Patch/Q259496/NT4/EN-US/Q259496i.exe | Microsoft NT Offload ModExpo Registry Permissions | Medium | Bug discussed in newsgroups and websites. |
| Microsoft[19]<br><br>Windows 95/98/2000 NT 4.0 | Internet Explorer 5.x | Internet Explorer allows circumventing "Cross frame security policy" by accessing the Document Object Model (DOM) of documents using Java/JavaScript. This gives a malicious user the ability to read local files, read files from any host, window spoofing, getting cookies, etc. | No workaround or patch available at time of publishing.<br><br>Unofficial workaround:<br>(Georgi Guninski Security Advisory #10, 2000)<br>Disable Active Scripting, including Java and JavaScript. | Microsoft JSObject Cross Frame Vulnerability | Medium | Bug discussed in newsgroups and websites. Exploit scripts have been published. |
| **Multiple Linux Vendors[20]**<br><br>***RedHat releases patches[21]***<br><br>***FreeBSD issues patches[22]*** | **Michael Sandrof IrcII 4.4-7 for S.u.S.E. Linux 6.3; RedHat Linux 6.1 i386** | **A buffer overflow exists in the DCC chat code that allows a remote malicious user to execute arbitrary code on a client's system.** | **Upgrade to IrcII version 4.4M: ftp://ircftp.au.eterna.com.au/pub/ircII/ircii-4.4M.tar.gz**<br><br>***Patches available at: (Please choose the proper version, [4.2, 5.2, 6.2] and architecture for your system)***<br>*ftp://updates.redhat.com/4.2/i386/ircii-4.4M-0.4.2.i386.rpm*<br><br>***Patches available at:***<br>ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/ | **IrcII DCC Chat Buffer Overflow** | **High** | **Bug discussed in newsgroups and websites. Exploit script has been published.** |

[18] Microsoft Security Bulletin, MS00-024, April 13, 2000.
[19] Securiteam, April 18, 2000.
[20] Securiteam, March 14, 2000.
[21] Red Hat Inc. Security Advisory, RHSA-2000:008-01, March 29, 2000.
[22] FreeBSD Security Advisory, FreeBSD-SA-00:11, April 10, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| Multiple Vendors[23]<br><br>Unix | RedHat Linux 6.x; XFree86 3.3.5-3.3.6, 4.0.0 | A Denial of Service vulnerability exists in the X11 font server shipped with RedHat Linux 6.x, which will prevent the X Server from functioning properly. This could result in remote root compromise. Similar problems also exist in the stock xfs. | No workaround or patch available at time of publishing. | Multiple Vendor X Font Server Denial of Service & Buffer Overflow | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Multiple Vendors[24]<br><br>Unix | GNU Emacs 20.0-20.6 | Several security vulnerabilities exist in Emacs and XEmacs, which could allow unprivileged local users, under certain conditions, the ability to eavesdrop on communication between Emacs and its subprocesses, and the ability to safely create temporary files in a public directory. | No workaround or patch available at time of publishing. | GNU EMACS 20 Vulnerabilities | Medium/ **High**<br><br>**(High in multi-user environ-ments)** | Bug discussed in newsgroups and websites. Exploit has been published. |
| Netscape[25] | Communi-cator 4.x | A vulnerability exists which will grant remote access to local html files (including the user's bookmark file and files in their cache) if both cookies and JavaScript are enabled. | No workaround or patch available at time of publishing.<br><br>Unofficial workaround: (SecurityFocus 2000-04-19) Disable cookies and JavaScript and make sure that the user profile is not named 'default'. | Netscape JavaScript-in-Cookies Vulnerability | Medium | Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the Press. |
| Novell[26] | Netware 5.1 (any system running on the top of Netware system with http remote administra-tion) | A Denial of Service security vulnerability exists which could allow a remote malicious user the ability to compromise the Administration utility to allow arbitrary code to be run on the server. | No workaround or patch available at time of publishing. | Netware 5.1 Remote Administration Buffer Overflow Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Panda Software[27]<br><br>Windows 9x | Panda Security 3.x | Several vulnerabilities exist, which could allow any local malicious logged-on user the ability to override his/her privileges, and the ability to become Administrator. | Patch available at: http://updates.pandasoftware.com/docs/us/Avoidvulnerability.zip | Panda Security 3.0 Multiple Vulnerabilities | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |

[23] Bugtraq, April 18, 2000.
[24] RUS-CERT Advisory, 200004-01, April 18, 2000.
[25] Securiteam, April 19, 2000.
[26] Bugtraq, April 18, 2000.
[27] DeepZone Security Advisory, April 17, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| QNX System Software, Limited (QSSL)[28]<br><br>Unix | QSSL QNX 4.25A | A vulnerability exists in the crypt() functionality, which allows the recovery of passwords from the hashes. This can result in the recovery of passwords by local users who have access to the password file, which in turn can result in the compromise of the root account. | No workaround or patch available at time of publishing. | QNX crypt() Vulnerability | Medium | Bug discussed in newsgroups and websites. Exploit script has been published. |
| Real Networks[29]<br><br>Windows, Unix | Real Server Pro, Intranet, Plus, Basic, 7.0, G2 1.0, | A Denial of Service vulnerability exists, which could allow a remote malicious user to cause the server to stop responding. | Patch now available. Please see RealServer Frequently Asked Questions at: http://service.real.com/help/faq/servg270.html | RealServer Port 7070 Denial of Service | Low/ **High**<br><br>**(High if DDoS best-practices not in place)** | Bug discussed in newsgroups and websites. Exploit scripts have been published. Vulnerability has appeared in the Press. |
| RedHat[30]<br><br>Unix | University of Washington imapd 12.264 | A buffer overflow vulnerability exists, which could allow a malicious user the ability to execute arbitrary code on the system; a valid login is required, however, and the code will execute only under the context of the valid login ID provided. | No workaround or patch available at time of publishing. | Univ. Of Washington imapd Buffer Overflow | Medium | Bug discussed in newsgroups and websites. |
| SGI[31]<br><br>Unix | IRIX 6.2-6.5.6 | Vulnerabilities exist in the Performance Copilot Package (PCP), which could allow anyone to perform queries by default. This exposes potentially sensitive information to anyone on the net. | No workaround or patch available at time of publishing. | IRIX Performance Copilot | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Sun Microsystems[32]<br><br>Unix | StarOffice 5.1 | A number of buffer overflow vulnerabilities exist, which could possibly allow the execution of arbitrary code. | No workaround or patch available at time of publishing. | Star Office Buffer Overflow Vulnerabilities | Medium | Bug discussed in newsgroups and websites. Exploit has been published. |
| Symantec[33]<br><br>Windows 95/98/ NT 4.0/2000 | PCAnywhere 32 8.0, 9.0 | It is possible for remote clients to cause a Denial of Service attack against the server. | No workaround or patch available at time of publishing. | PCAnywhere Denial of Service | Low | Bug discussed in newsgroups and websites. Exploit has been published. |

[28] Bugtraq, April 14, 2000.
[29] USSR Advisory Code, USSR-2000038, April 20, 2000.
[30] Securiteam, April 20, 2000.
[31] Bugtraq, April 12, 2000.
[32] Securiteam, April 19, 2000.

| Hardware/ Operating System/ Vendor | Equipment/ Software Name | Vulnerability/ Impact | Patches/Workarounds/Alerts | Common Name | Risk* | Attacks/Scripts |
|---|---|---|---|---|---|---|
| TalentSoft, Inc.[34]<br><br>Unix | Web+ 4.x | A directory traversal vulnerability exists, which could allow malicious users to read arbitrary data files on the server. | Patch to resolve this issue in builds 512 and previous are available at: ftp://ftp.talentsoft.com/Download/Webplus/Unix/webplus46p%20Read%20me.html | TalentSoft Web+ Directory Traversal | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| TrendMicro Systems[35]<br><br>Windows NT | Interscan version V3.32, build 1011, 1022 | A Denial of Service vulnerability exists which could allow a malicious user to crash the SMTP service. | Version 3.25 lacks a few of the features of version 3.32 - but is also is not subject to the DoS exploits found in version 3.32. | TrendMicro Denial of Service | Low/ **High**<br><br>**(High if DDoS best-practices not in place)** | Bug discussed in newsgroups and websites. Exploit has been published. |
| TurboLinux[36]<br><br>Unix | TurboLinux versions: 6.0.2 and earlier | A vulnerability exists in the PAM package, which could allow local malicious users to gain root privileges. | Updated package available at: ftp://ftp.turbolinux.com/pub/updates/6.0/security/pam-0.72-3.i386.rpm | TurboLinux PAM Vulnerability | **High** | Bug discussed in newsgroups and websites. Exploit has been published. |
| University of Washington[37]<br><br>Unix | imapd 12.264<br><br>(This version is shipped with RedHat Linux 6.2) | A buffer overflow vulnerability exists in the list command, which could allow the execution of arbitrary code. This vulnerability would only be useful in a scenario where a user has an account, but no shell level access. This would allow them to gain shell access. | No workaround or patch available at time of publishing. | Univ. Of Washington imapd Buffer Overflow | Medium | Bug discussed in newsgroups and websites. |

*Risk is defined in the following manner:

**High -** A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

**Medium -** A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

**Low** - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

---

[33] Bugtraq, April 10, 2000.
[34] Sword & Shield Enterprise Security, Inc. Security Advisory, April 12, 2000.
[35] Bugtraq, April 17, 2000.
[36] Turbo Linux Security Announcement, TLSA2000009-1, April 14, 2000.
[37] SecurityFocus, April 20, 2000.

## *Recent Exploit Scripts/Techniques*

The table below contains a representative sample of exploit scripts and How to Guides, identified between April 6 and April 20, 2000, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period,50 scripts, programs, and net-news messages containing holes or exploits were identified.

| **Date of Script** (Reverse Chronological Order) | **Script Name** | **Script Description** |
|---|---|---|
| **April 19-20, 2000** | **Bedie.tar.gz** | **BeOS local Denial of Service exploit script.** |
| **April 19-20, 2000** | **Bizdb.htm** | **Remote exploit for the BizDB vulnerability.** |
| April 19-20, 2000 | Ide_expl.mrc | An IRCii-4-4 exploit ported to mirc5.7. |
| April 19-20, 2000 | Imap_core.sh | Quick proof-of-concept tool that causes some imapd implementations to dump core. |
| April 19-20, 2000 | Lincity.c | Local buffer overflow exploit. |
| April 19-20, 2000 | Lprm-bsd.c | Exploit script for the lprm local root vulnerability in OpenBSD and FreeBSD stable. |
| **April 19-20, 2000** | **Ltrust.c** | **Linux kernel 2.2.14 local Denial of Service exploit script.** |
| **April 19-20, 2000** | **Named_dump.sh** | **ISC BIND 4.9.7-T1B local exploit script.** |
| April 19-20, 2000 | Nessus-1.0.0pre2.tar.gz | Full-featured remote security scanner for Linux, BSD, Solaris, and some other systems which is multi-threaded, plugin-based, with a nice GTK interface and currently performs over 330 remote security checks. |
| April 19-20, 2000 | RFP2K03.txt | Perl exploit script for the Microsoft DVWSSR.DLL vulnerability. |
| April 19-20, 2000 | Sersniff-0.0.3.tar.gz | Program for tunneling/sniffing between two serial ports, which was written to help aid with the decoding of the protocol for the Nokia 9000I Communicator. |
| April 19-20, 2000 | Vtun-2.1.tar.gz | Vtun is the easiest way to create Virtual Tunnels over TCP/IP networks with traffic shaping, compression, and encryption. |
| April 19-20, 2000 | Wakeonlan.pl | Perl script that sends 'magic packets' to wake-on-lan enabled Ethernet adapters in order to remotely power up a PC. |
| April 17-18, 2000 | Bsyrin1.zip | Tool for checking servers/daemons for buffer overflows on given parameters, which has a flexible configuration file where you input the parameters needed to run the program. |
| April 17-18, 2000 | Communicate.pl | Denial of Service exploit script for the CommuniGatePro 3.1 NT vulnerability. |
| April 17-18, 2000 | Netsurfer.txt | Technique for local users on how to steal credit card numbers and personal information from a Netsurfer e-commerce site. |
| April 17-18, 2000 | Nmap-12b-1.3.tar | Web interface to nmap that allows you to submit nmap commands and receives responses. |
| April 17-18, 2000 | R00tlate.pl | Perl script to grab a list of new files from r00tabega.com which then gives the user the ability to pick and download any of the files. |
| **April 17-18, 2000** | **RDS_Toolkit.zip** | **Another add-on for Msadc.pl that spawns a remote command on Windows and Unix based syringe using RDS.** |
| April 17-18, 2000 | Saint-2.0.1.tar.gz | Security assessment tool based on SATAN. |
| **April 13-16, 2000** | **Dnshack.pl** | **Remote NT exploit script.** |
| April 13-16, 2000 | Nbnbs.c | NetBIOS name bulk security scanner for Unix which does long-range network scans for NetBIOS names and logs positives. |
| April 13-16, 2000 | RFP2K02.txt | "Netscape engineers are weenies!" AKA a backdoor in Microsoft FrontPage extensions/authoring components. Includes a dvwssr.pl Perl-based exploit script. |
| **April 11-12, 2000** | **Cryptc41.c** | **Unix exploit for CRYPTOCards's vulnerability.** |

| Date of Script (Reverse Chronological Order) | Script Name | Script Description |
|---|---|---|
| **April 11-12, 2000** | **DeCRYPTO.zip** | **Windows 9x demonstration exploit for CRYPTOCards's vulnerability.** |
| April 11-12, 2000 | Fortres4-analysis.txt | Security software for Windows which has an easily decrypted password. |
| April 11-12, 2000 | Nessus-1.0.0pre1.tar.gz | Full-featured remote security scanner for Linux, BSD, Solaris and some other systems which performs over 330 remote security checks. |
| April 11-12, 2000 | Nmap-2.30BETA20.tgz | Advanced utility for network exploration or security auditing, which supports ping scanning, many port scanning techniques, TCP/IP fingerprinting, advanced host enumeration, firewall bypassing and more. |
| April 11-12, 2000 | Sourcegrab.pl | Exploit script for the Microsoft Index Server 2.0 hit highlight vulnerability. |
| April 11-12, 2000 | Winfingerprint-224.zip | Advanced remote Windows OS detection. |
| April 8-10, 2000 | Apsend.tar.gz | TCP/IP packet sender to test firewalls and other network applications which includes a syn flood option, land Denial of Service attack, Denial of Service attack against tcpdump3.4, and spoofing. |
| April 8-10, 2000 | Cattscanner-0.61.tar.gz | Configurable Autonomous Threaded Topography scanner is a compilation of common networking tools. |
| April 8-10, 2000 | Cool.txt | Exploit details for the Netscape PublishingExpert 2.x file-reading/dir-listing vulnerability. |
| April 8-10, 2000 | Dsniff-1.8.tar.gz | A suite of utilities that are useful for penetration testing. |
| April 8-10, 2000 | Nmap-2.30BETA19.tgz | Advanced utility for network exploration or security auditing which supports ping scanning, many port scanning techniques, TCP/IP fingerprinting, etc. |
| April 8-10, 2000 | Nscan666.zip | Fast and flexible Windows portscanner that is designed for scanning large networks and gathering related network/host information. |
| April 8-10, 2000 | Sara-2.1.13.tar.gz | Security analysis tool based on the SATAN mode. |
| April 6-7, 2000 | Ircii-4.4.c | Buffer overflow exploit which allows the execution of arbitrary code. |
| April 6-7, 2000 | Ms00-019.info.txt | Exploit information for the Virtualized UNC Shares vulnerability. |
| April 6-7, 2000 | q-2.0.tgz | Client/server backdoor which features remote shell access with strong encryption for root and normal users, and an encrypted on-demand TCP relay/bouncer that supports encrypted sessions with normal clients using the included tunneling daemon. |
| April 6-7, 2000 | Rmp_query.c | Exploit script for the Caldera OpenLinux 2.3 vulnerability. |
| April 6-7, 2000 | Sentinel-0.6.tar.gz | The Sentinel project is designed to be a portable accurate implementation of all publicly known promiscuous detection techniques. |
| **April 20, 2000** | **Realdie.exe** | **Exploit script for the RealServer Port 7070 Denial of Service vulnerability.** |
| **April 20, 2000** | **Realdie.zip** | **Exploit script for the RealServer Port 7070 Denial of Service vulnerability.** |
| **April 18, 2000** | **jsinject.java** | **Exploit technique for Microsoft JSObject Cross Frame vulnerability.** |
| **April 18, 2000** | **Kill_nwtcp.c** | **Exploit script for the Netware 5.1 Remote Administration Buffer Overflow vulnerability.** |
| **April 18, 2000** | **Kill-xfs.c** | **Multiple Vendor X Font Server Denial of Service & Buffer Overflow vulnerability exploit.** |
| **April 18, 2000** | **Sinject.html** | **Exploit technique for Microsoft JSObject Cross Frame vulnerability.** |
| April 17, 2000 | No_reg.zip | Exploit script for the Panda Security 3.x vulnerabilities. |
| **April 14, 2000** | **Decrypt-qnx.c** | **Exploit script for the QNX vulnerability.** |

## *Script Analysis*

When available, this section will supply a short description of scripts that have been analyzed by various security professionals and organizations. **We encourage you or your organization to contribute.** If you wish to do so, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While space constraints may limit the length of description included in this document, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

## *Trends*

**DDoS/DoS:**

- An increase in alteration of delegated nameserver information for domain names causing DNS-based Denial of Service.

**Probes/Scans:**

- **A how-to has been published on the AMDROCKS BIND exploit.**
- **An increase in exploiting the rpc.sadmind vulnerability.**
- **An increase from Brazil in exploits and scans to port 53 are being used against well-known vulnerabilities, the NXT overflow vulnerability, which creates the directory ADMROCKS after entry, and the BIND vulnerability.**
- An increase scans on port 27063.
- An increase in scans on Port 98 (linuxconf).
- There has been an increase in probes to UDP Port 137 (NetBIOS Name Service)**.**
- An increase in probes to port 1080/tcp (RingZero Trojan) and port 1243 (SubSeven Trojan).
- There has been an increase in port scans from Argentina and an increase in scans from Korean hosts that are aimed at ports 111, 2974, and 4333. There has also been are reported increase in probes on ports 1080, 1953, and 31337. An increase in probes to ports 109/tcp, 137/udp, 138/udp, and 139/tcp has also been reported.

**Other:**

- ***The CIH (Chernobyl) virus, the most destructive virus ever, will activate on April 26!***
- **An increase in reports of intruders exploiting unprotected Windows networking shares.**
- Exploits are being used against the Irix objectserver vulnerability.
- An increase in exploitation of unprotected Windows networking shares.
- Exploits are still being used against well-known vulnerabilities, the RDS DataFactory object and Microsoft IIS web servers, which is a component of Microsoft Data Access Components (MDAC).
- Reports indicate registry objects being maliciously altered which include: point of contact information for domain names, IP address delegations, and autonomous system numbers.
- Forged email headers are being used to bypass weak registry transaction authentication mechanisms.
- There has been an increase in the recent distribution of worm variants of Melissa and PrettyPark.

## *Viruses*

A list of viruses infecting two or more sites as reported to various anti-virus vendors has been categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages, as updates become available**. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections during the last three months reported), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. These types of malicious code will now be included in the table where appropriate.

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **203** distinct viruses are currently consider "in the wild" by anti-virus experts with another **328** viruses suspected to be in the wild. In the wild viruses have been reported to anti-virus vendors by their clients and have infected user machines. The suspected in the wild number is derived from reports by a single source.

| Ranking | Common Name | Type of Code | Trends | Date |
|---|---|---|---|---|
| 1 | W32/SKA (aka Happy 99) | File | Increase | March 1999 |
| 2 | W32 PrettyPark | File | Increase | June 1999 |
| 3 | W97M Ethan.A | Macro | Steady | February 1999 |
| 4 | W97M Marker | Macro | Slight decrease | August 1998 |
| 5 | VBS/Kakworm | Script | New to table | December 1999 |
| 6 | W95 CIH | File | Slight decrease | April 1999 |
| 7 | VBS/Freelink | Script | New to table | July 1999 |
| 8 | XM Laroux | Macro | New to table | April 1996 |
| 9 | W97M Melissa.A | Macro | Decrease | April 1999 |
| 10 | O97M Tristate | Macro | New to table | April 1999 |

**PE-CIH (CIH, Chernobyl, Win95.CIH, Win32.CIH, W95.CIH V1.2, W95.CIH V1.3, W95.CIH V1.4) (File Infector Virus): The most destructive virus ever is programmed to activate on April 26!** When PE_CIH activated in 1999, it caused damage to several hundred thousand systems.

This virus contains two destructive payloads, which will both trigger on April 26th. Once triggered, it attempts to overwrite the system's hard disk with some random data, which makes data recovery very difficult. It also tries to do some permanent damage to the system by corrupting data stored in the Flash BIOS. Once it reformats the hard drive it displays a text message. It does not infect Windows NT systems.

**W97M/Appder.A:** This virus consists of three macros called AUTOOPEN, AUTOCLOSE and APPDER. On opening a document the virus checks to see if it contains any of the two macros, and if neither of them exists, it infects this document.

W97M/Appder.A uses the WINDOWD6.INI file for housing the NTTHNTA variable, which will be used as a counter to store the number of documents opened. When this counter reads "20" the destructive payload of the virus is activated. This consists in the deletion of all files with EXE extension that are found

in the C:\DOC directory. It will also delete all COM and EXE files in the C:\WINDOWS directory and all .TTF and .FOT files in the C:\WINDOWS\SYSTEM directory.

**WM97/Astia-AI (W97M/Titastic) (Word 97 Macro Virus):** This virus has been reported in the wild. It creates two infected files (BOOK.DOT and BOOK.SRC) in Microsoft Word's StartUp directory as well as infecting Word's global template NORMAL.DOT.

All three files need to be disinfected. Sophos Anti-Virus's on-demand scanner does not check SRC files by default, so if an infection of WM97/Astia-AI is found you should enable the "Scan all file types" option.

A message box with the title 'TITANUS' is displayed if you enter the Visual Basic Editor on an infected machine. If you press 'Yes' then the text 'Macro non-TITANUS' is inserted into the open document.

**WM97/Bridge-A (Word 97 Macro Virus):** This virus has been reported in the wild. It contains two macros called Contec and MdCont. The virus changes the Event name that it runs from into Acol. This is done in an attempt to avoid detection.

**W97M_Class.El (Aliases: Class.El) (Word 97 Macro Virus):** This is a Word 97 Macro virus that replicates using its own module residing in the ThisDocument stream. If the current system year is 2001, a message box is displayed.

**W97M_Doghack.A (Aliases: Doghack.A, W97m/Doghack.A) (Word 97 Macro Virus):** When run, this virus modifies some menu items to disallow the user from seeing the viral code. It is triggered on a Wednesday, when it displays a text message and deletes the infected document's organizer.

**W97M_Hope.U (Aliases: Hope.U) (Word 97 Virus):** This virus stores itself in the ThisDocument module. Then it checks if the active document or the normal template is infected, by comparing the codes in the ThisDocument module to the viral code. If the code in the ThisDocument module of the active document or normal template is equal to the viral code for W97M_HOPE.U, the virus deletes the code in the ThisDocument module, copies its viral code in the ThisDocument module, and then saves itself. The infected ThisDocument module contains the string: "Rachel Is A Hottie!"

The virus, like other macro viruses, also disables the macro virus protection. It also disables the Cancel Key, including the Prompting to save the Normal Template.

**WM97/IIS-E (Word 97 Macro Virus):** This virus has been seen in the wild. It is a polymorphic macro virus that uses randomly created variable names.

**WM97/Locale-D (Word 97 Macro Virus):** This virus has been reported in the wild. It is a combination of two viruses: WM97/Locale-A and WM97/Marker.

This combined virus has the same payload as WM97/Marker. Whenever a document is closed, the virus takes the information in File|Properties|Summary and ftps it to the Codebreakers site. It also attaches the sent information to the bottom of the infected macro as comments.

**WM97/Marker-C (Word 97 Macro Virus):** This virus has been seen in the wild. Whenever a document is closed the virus takes the information in File|Properties|Summary, and ftps it to the Codebreakers website. It also attaches the sent information to the bottom of the macro as a comment.

**WM97/Marker-CI (Word 97 Macro Virus):** This virus has been reported in the wild and is a variant of the WM97/Marker Word macro virus. The virus code contains the following text, which does not get displayed: Virus Created By An Indian Citizen.

**WM97/Marker-DB (Word 97 Macro Virus):** This virus has been reported in the wild and is a variant of the WM97/Marker Word macro virus. It attempts to send user data such as name, address, date and time of the document infection to the Codebreakers FTP site.

**WM97/Marker-DD (Word 97 Macro Virus):** This virus has been reported in the wild and is a variant of the WM97/Marker Word macro virus. The virus changes the user information settings.

UserName becomes fs080298
UserInitials becomes FS2000
UserAddress becomes fs080298@hotmail.com

The virus also creates an HTML file called EmailMe.html in the root directory, and sets it as Windows wallpaper.

**W97M/Marker.E:** When this virus enters the system, it checks to see if the NORMAL.DOT global template is infected by looking for the text string "Marker" in it. If it is found, it means that the template is already infected and the virus will not re-infect it. Next, it disables the antivirus protection in macros.

On any day of the month, W97M/Marker.E should create two files in the root directory, HSFxxxx.SYS and NETLDx.VXD. The former contains the files of the virus code itself whereas the latter contains a text that permits executing the commands it contains through the FTP.EXE application, but only after an MS-DOS session has been opened. This way, the virus manages to send the data about each user infected until then to a certain address.

**WM97/Melissa-AU (Aliases: Elecciones.A, Elecciones2000, W97M/Elecciones2000) (Word 97 Macro Virus and E-Mail Worm):** This virus is a variant of the WM97/Melissa Word macro virus. It sends itself to the first 50 people in each Outlook address book. Depending on the date, the message subject is either "Elecciones 2000: ultima encuesta Apoyo!" or "Urgente: Confirmar!". On 9 April the virus attempts to delete all files from drives C: to Z:.

The virus appears to have been written as a reaction to recent elections in Peru. Because the virus forwards itself using Spanish phrases it is unlikely to successfully spread in non-Spanish speaking countries.

**WM97/Murke-A (Word 97 Macro Virus):** This virus has been reported in the wild and is a very simple Word macro virus, which contains three commented-out Russian e-mail addresses.

**WM97/Thursday-U (Word 97 Macro Virus):** This virus has been reported in the wild and is a variant of the WM97/Thursday Word macro virus. This variant does not contain the destructive payload that is included in other Thursday variants.

**W97M_NOARMY (Polymorphic Macro Virus):** This virus was recently reported in Europe. It is not destructive, however it tries to modify the active document and also tries to e-mail itself to 50 addresses in the Microsoft Outlook address book of the infected user. While most viruses use the same subject line and message body, W97M_NOARMY has the ability to use different text for the subject line and message body.

**TROJ_JANE.B (Worm):**. TROJ_JANE.B spreads through mIRC by sending an infected file (filename: Jane.BMP.Exe) to all users in the active chat channel. Due to its filename many users believe that they have received an image (by default Microsoft Windows hides file extensions for known file types, the file appears as "Jane.BMP"). Once a user double-clicks on the file, TROJ_JANE.B copies itself to the Windows system directory and then modifies the Windows registry to that it is activated every time the computer is rebooted. While TROJ_JANE.B does not contain any destructive payload, it can be used by a hacker to collect user information.

# *Trojans*

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. The increasing number of Trojans gains added significance due to recent testing conducted to determine the ability of anti-virus software to detect Trojans. According to the test results, a number of popular anti-virus products failed to detect or had limited detection capabilities against current popular Trojans. Testing also indicates that detection of a baseline Trojan does not necessarily mean the anti-virus software can detect a variant. Readers should contact their anti-virus vendors to obtain specific information on Trojans and their variants that their software detects.

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #2000-01 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

***There are no new Trojans to report in this issue of CyberNotes.***

| Trojan | Version | Issue Discussed |
|---|---|---|
| Acid Shiver + lmacid | v1.0 + 1.0Mod | CyberNotes-2000-07 |
| AOL Trojan | | CyberNotes-2000-01 |
| Bla | 1.0-5.02 | CyberNotes-2000-06 |
| DeepThroat | v1.0 - 3.1 + Mod (Foreplay) | CyberNotes-2000-05 |
| Delta Source | J0.5b-0.7 | CyberNotes-2000-01 |
| Donald Dick | 1.52-1.55 | CyberNotes-2000-01 |
| FakeFTP | Beta | CyberNotes-2000-02 |
| Girlfriend | V1.3x (including Patch 1 & 2) | CyberNotes-2000-05 |
| Hack`a`Tack | 1.2-2000 | CyberNotes-2000-06 |
| Hack'A'tack | 1.0-2000 | CyberNotes-2000-01 |
| ik97 | v1.2 | CyberNotes-2000-07 |
| InCommand | 1.0-1.4 | CyberNotes-2000-01 |
| Infector | v1.3 | CyberNotes-2000-07 |
| Intruder | | CyberNotes-2000-01 |
| Kuang Original | 0.34 | CyberNotes-2000-01 |
| Matrix | 1.4-2.0 | CyberNotes-2000-01 |
| MoSucker | | CyberNotes-2000-06 |
| NetController | v1.08 | CyberNotes-2000-07 |
| NetSphere | v1.0 - 1.31337 | CyberNotes-2000-06 |
| NetTrojan | 1.0 | CyberNotes-2000-06 |
| Nirvana / VisualKiller | v1.94 - 1.95 | CyberNotes-2000-07 |
| Prayer | 1.2-1.3 | CyberNotes-2000-06 |
| Setup Trojan (Sshare) +Mod Small Share | | CyberNotes-2000-06 |
| ShadowPhyre | v2.12.38 - 2.X | CyberNotes-2000-06 |
| Softwarst | | CyberNotes-2000-05 |
| SubSeven | 1.0-2.1c | CyberNotes-2000-01 |
| SubSeven | 1.0-2.1Gold | CyberNotes-2000-02 |
| SubSeven | V1.0-1.9b, v2.1+SubStealth, v2.2b1 | CyberNotes-2000-07 |
| Trinoo | | CyberNotes-2000-05 |
| TryIt | | CyberNotes-2000-05 |
| wCrat | v1.2b | CyberNotes-2000-05 |